Method for verifying the validity of digital franking notes

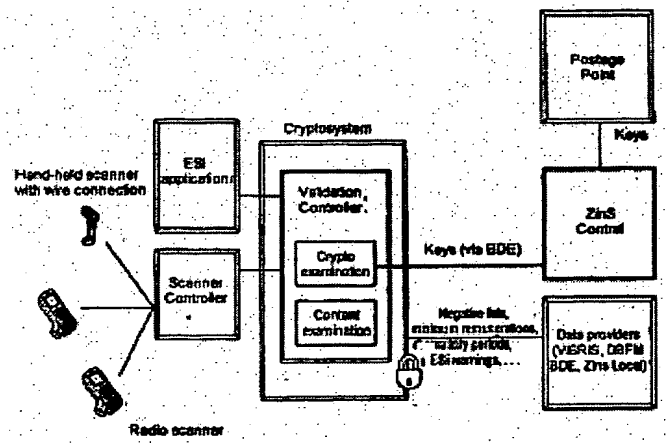
Patent number: DE10131254
Publication date: 2003-01-23
Inventor: DELITZ ALEXANDER (DE); FERY PETER (DE); HELMUS JUERGEN (DE); HOEHL ALOYSIUS (DE); MEIER GUNTHER (DE); ROBEL ELKE (DE); STUMM DIETER (DE)
Applicant: DEUTSCHE POST AG (DE)
Classification:
- international: *G07B17/00;* **G07B17/00;** (IPC1-7): H04L9/00; G06K9/18
- european: G07B17/00E4; G07B17/00F3
Application number: DE20011031254 20010701
Priority number(s): DE20011031254 20010701

Also published as:
WO03005307 (A1)
EP1405274 (A1)
US2004249764 (A1)
CN1554076 (A)
CA2452750 (A1)

Report a data error here

Abstract of **DE10131254**

The invention relates to a method for verifying the authenticity of a franking note placed on a postal article. According to the invention, cryptographic information contained in the franking note is decoded and used for verifying the authenticity of the franking note. The inventive method is characterized in that the reading unit graphically records the franking note and transmits it to a verification unit and in that the verification unit controls a sequence of partial tests.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 31 254 A 1**

(51) Int. Cl.[7]:
H 04 L 9/00
G 06 K 9/18

(21) Aktenzeichen: 101 31 254.7
(22) Anmeldetag: 1. 7. 2001
(43) Offenlegungstag: 23. 1. 2003

(71) Anmelder:
Deutsche Post AG, 53175 Bonn, DE

(74) Vertreter:
Jostarndt Thul Patentanwälte, 52074 Aachen

(72) Erfinder:
Delitz, Alexander, 53177 Bonn, DE; Fery, Peter, 64673 Zwingenberg, DE; Helmus, Jürgen, 53229 Bonn, DE; Höhl, Aloysius, 36041 Fulda, DE; Meier, Gunther, 64354 Reinheim, DE; Robel, Elke, 59368 Werne, DE; Stumm, Dieter, 26629 Großefehn, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 198 12 902 A1
EP 03 60 225 B1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Überprüfen der Gültigkeit von digitalen Freimachungsvermerken

(57) Die Erfindung betrifft ein Verfahren zur Überprüfung der Echtheit eines auf einer Postsendung aufgebrachten Freimachungsvermerks, wobei in dem Freimachungsvermerk enthaltene kryptographische Informationen entschlüsselt und zur Überprüfung der Echtzeit des Freimachungsvermerkes eingesetzt werden.
Erfindungsgemäß zeichnet sich das Verfahren dadurch aus, dass die Leseeinheit den Freimachungsvermerk graphisch erfasst und an eine Überprüfungseinheit übermittelt und dass die Überprüfungseinheit einen Ablauf von Teilprüfungen steuert.

DE 101 31 254 A1

DE 101 31 254 A1

Beschreibung

[0001] Es ist bekannt, Postsendungen mit digitalen Freimachungsvermerken zu versehen.

[0002] Um den Absendern der Postsendungen die Erzeugung der Freimachungsvermerke zu erleichtern, ist es beispielsweise bei dem von der Deutschen Post AG eingesetzten Frankierungssystem möglich, Freimachungsvermerke in einem Kundensystem zu erzeugen und über eine beliebige Schnittstelle auf einen Drucker auszugeben.

[0003] Um einen Missbrauch dieses Verfahrens zu vermeiden, enthalten die digitalen Freimachungsvermerke kryptographische Informationen, beispielsweise über die Identität des die Erzeugung des Freimachungsvermerkes steuernden Kundensystems.

[0004] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zu schaffen, mit dem die Echtheit der Freimachungsvermerke schnell und zuverlässig überprüft werden kann. Insbesondere soll sich das Verfahren für eine Überprüfung in einem Großserieneinsatz, insbesondere in Brief- oder Frachtzentren, eignen.

[0005] Erfindungsgemäß wird diese Aufgabe dadurch gelöst, dass die Leseeinheit den Freimachungsvermerk graphisch erfasst und an eine Überprüfungseinheit übermittelt, und dass die Überprüfungseinheit einen Ablauf von Teilprüfungen steuert.

[0006] Es ist besonders zweckmäßig, dass eine der Teilprüfungen die Entschlüsselung der in dem Freimachungsvermerk enthaltenen kryptographischen Informationen beinhaltet.

[0007] Durch die Integration der Entschlüsselung der kryptographischen Informationen in den Prüfungsprozess ist es möglich, die Echtheit der Freimachungsvermerke unmittelbar zu erfassen, so dass eine Überprüfung online – insbesondere während des Bearbeitungsverlaufs der Postsendung in einer Bearbeitungsmaschine – erfolgen kann.

[0008] Ferner ist es vorteilhaft, dass eine der Teilprüfungen einen Vergleich zwischen dem Erzeugungsdatum des Freimachungsvermerks und dem aktuellen Datum beinhaltet. Die Integration des Erzeugungsdatums des Freimachungsvermerks – insbesondere in verschlüsselter Form – erhöht die Datensicherheit, da durch den Vergleich zwischen dem Erzeugungsdatum des Freimachungsvermerkes und dem aktuellen Datum eine mehrfache Verwendung eines Freimachungsvermerks zur Beförderung von Postsendungen vermieden wird.

[0009] Zur weiteren Erhöhung der Überprüfungsgeschwindigkeit ist es vorteilhaft, dass die Leseeinheit und die Überprüfungseinheit mittels eines synchronen Protokolls Informationen austauschen.

[0010] In einer anderen, gleichfalls zweckmäßigen Ausführungsform der Erfindung, kommunizieren die Leseeinheit und die Überprüfungseinheit über ein asynchrones Protokoll miteinander.

[0011] Hierbei ist es besonders zweckmäßig, dass die Leseeinheit ein Datentelegramm an die Überprüfungseinheit sendet.

[0012] Vorzugsweise enthält das Datentelegramm den Inhalt des Freimachungsvermerks.

[0013] Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Zeichnungen.

[0014] Von den Zeichnungen zeigen

[0015] Fig. 1 eine Prinzipdarstellung von Systemkomponenten eines Entgeltsicherungssystems;

[0016] Fig. 2 eine besonders bevorzugte Ausführungsform des Entgeltsicherungssystems, Handscanner und Entgeltsicherungs-PC);

[0017] Fig. 3 eine Prinzipdarstellung einer Erzeugung und Überprüfung von Freimachungsvermerken.

[0018] Fig. 4 eine Übersicht über Komponenten des Krypto-Systems;

[0019] Fig. 5 eine bevorzugte Durchführungsform des Überprüfungsverfahrens;

[0020] Fig. 6 eine weitere besonders bevorzugte Ausführungsform des Überprüfungsverfahrens mit einem besonders bevorzugten Ablauf von Teilprüfungen;

[0021] Fig. 7 einen bevorzugten Ablauf einer Verteilung von Schlüsseln zwischen einer zentralen Ladestelle (Postage Point) und einzelnen kryptographischen Überprüfungseinheiten (Crypto Server).

[0022] Nachfolgend wird die Erfindung am Beispiel eines PC-Freimachungssystems dargestellt. Die zur Entgeltsicherung dienenden Verfahrensschritte sind dabei unabhängig von dem zur Erzeugung der Freimachungsvermerke eingesetzten System.

[0023] Die dargestellte dezentrale Überprüfung an einzelnen Kontrollstellen, insbesondere in Briefzentren, ist besonders bevorzugt, jedoch ist eine zentralisierte Überprüfung gleichermaßen möglich.

[0024] In einer ersten Ausführungsform der Erfindung erfolgt vorzugsweise eine Überprüfung der Echtheit der Freimachungsvermerke stichprobenweise durch einzelne Scanner.

[0025] Ein hierzu geeignetes Überprüfungssystem enthält vorzugsweise die in Fig. 1 dargestellten Komponenten.

[0026] In Fig. 1 ist dargestellt, mit welchen Teilsystemen das Krypto-System in Beziehung steht. Sie werden im Folgenden kurz beschrieben.

Scanner

[0027] Die Scanner dienen zum Einlesen des Frankierungsvermerks der PC-Frankierung. Bei den Frankierungsvermerken handelt es sich um 2D-Codes im Format Datamatrix, mit der verwendeten Fehlerkorrektur ECC200. Je nach Scannertyp werden die Daten per Funk oder per Kabel übertragen, wobei die Funkscanner über ein mehrzeiliges Display und damit über eine Ausgabemöglichkeit und einen Touchscreen, beziehungsweise eine Tastatur zur rudimentären Eingabe verfügen. Die Schnittstelle zwischen den Scannern und den restlichen Systemen des bevorzugten Entgeltsicherungs-PC-Frankierung-Systems bilden der Scanner Controller und der Validation-Controller als Komponenten. Während der Scanner-Controller eine Queue von Matrixcodes verwaltet, die über den Handscanner kommend zur Prüfung anstehen und im Wesentlichen den Kontakt zu den Scannern aufrechterhalten, ist er mit den weiteren System nur über den Validation-Scanner in Kontakt.

Scanner Controller/Validation-Controller

[0028] Scanner Controller, beziehungsweise Validation-Controller, dienen als Schnittstelle zwischen den Scannern und den weiteren Systemen zur Überprüfung der 2D-Barcodes. Ihnen wird der aus der optischen Erfassung umgewandelte und fehlerkorrigierte 2D-Barcodeinhalt übermittelt, und sie veranlassen daraufhin die Überprüfung und sorgen im Falle der Funkscanner für eine Ausgabe des Lese- und Prüfergebnisses, und dienen als Schnittstelle zwischen eventuell notwendigen manuellen Nachbearbeitungen und Prüfungen des Prüfers und den übrigen Systemen.

Krypto-System

[0029] Das Krypto-System sorgt für die inhaltliche und kryptographische Überprüfung des 2D-Barcodeinhaltes sowie für die geschützte Speicherung sicherheitsrelevanter Daten und Algorithmen. Auf die einzelnen Komponenten wird später eingegangen.

Gebührenbetragsladestelle (Postage Point)

[0030] Die Gebührenbetragsladestelle (Postage Point) ist das zentrale System innerhalb der PC-Frankierung. Sie dient als Schnittstelle zu den Kundensystemen. Von ihr können die Kunden Vorgabebeträge zur anschließenden Frankierung entladen. Auf der Gebührenbetragsladestelle (Postage Point) werden die Schlüssel zur Absicherung des Verfahrens generiert. Ferner dient sie als Schnittstelle zu den Abrechnungs-Systemen. Folgende Schnittstellen werden zu dem bevorzugten Entgeltsicherungssystem zur PC-Frankierung bereitgestellt:

- Sendungsinformationen über den 2D-Barcode
- Symmetrische Schlüssel
- Stammdaten, wie zum Beispiel Vorgabebeträge, Kontostände

Bevorzugte Entgeltsicherung Zentral

[0031] In dem bevorzugten Entgeltsicherungs-Zentral-System werden die sendungsbezogenen Informationen gesammelt und anderen Systemen zur Verfügung gestellt. Hier findet die Erstellung der Produktionsberichte statt, die wiederum zur Erstellung der Negativdateien führen. Weiterhin erhält das Entgeltsicherungs-Zentral-System von der Gebührenbetragsladestelle (Postage Point) die aktuellen Schlüsseldaten und leitet diese an die einzelnen Krypto-Server weiter.

Datenlieferanten

[0032] Zur inhaltlichen Überprüfung der 2D-Barcodes sind eine Reihe von Stammdaten notwendig, wie zum Beispiel Negativdateien, Mindestentgelte, Gültigkeitszeiträume in Relation zu dem Produkt und Entgeltsicherung-Warnungs- und Folgeverarbeitungscodes. Diese Daten werden aus unterschiedlichen Systemen (BDE, VIBRIS, lokales Entgeltsicherungs-System) bereitgestellt.

Entgeltsicherung-Anwendung

[0033] Mit der Entgeltsicherung-Anwendung hat der AGB-Prüfer, der die ausgeschleusten PC-Freimachungs-Sendungen nachbearbeiten muss, die Möglichkeit, eine detailliertere Überprüfung der Frankierung vorzunehmen, bei der die Darstellung der Prüfergebnisse nicht durch begrenzte Ausgabemöglichkeiten des Scanners eingeschränkt wird. Zusätzlich kann der Prüfer hier auch weitere Daten, wie den Gültigkeitszeitraum des Portobetrages, auf welchen sich die aktuelle Sendung bezieht, sowie den Betrag und die in Anspruch genommenen Frankierungen einsehen.

Automatische Erfassung der 2D-Barcodes

[0034] Die automatische Erfassung der 2D-Barcodes erfolgt innerhalb der SSA. Hierzu werden die Bildinformationen an den AFM-2D-Code-Leser weitergeleitet. Dort erfolgt die Konvertierung des Bildes in den Inhalt des Datamatrixcodes. Im Anschluss daran wird der 2D-Barcodeinhalt an das Krypto-System zur Prüfung übermittelt, das zurückgegebene Prüfergebnis ausgewertet und an das optische Erfassungssystem (IMM) zur Codierung der Sendung übermittelt. Bevorzugte Bestandteile eines derart erweiterten Überprüfungsverfahrens sind in Fig. 2 dargestellt.

AFM-2D-Code-Leser

[0035] Pro Lesemaschine (ALM/ILVM) existiert ein AFM-2D-Code-Leser, der über ein optisches Erfassungssystem (IMM) die Bilddaten der Sendungen erhält und für Entgeltsicherungszwecke weiter verarbeitet. Im Rahmen von bevorzugter Entgeltsicherungs-PC-Frankierung bedeutet dies im Falle eines erkannten 2D-Codes, dass aus den Bilddaten der 2D-Datamatrixcode extrahiert und unter Zuhilfenahme des Fehlerkorrekturverfahrens ECC200 in eine Bytekette umgewandelt wird, die den Inhalt des 2D-Barcodes darstellt.

[0036] Diese Bytekette wird an den Validation Controller zur Überprüfung übergeben. Das Prüfergebnis wird anschließend über die Schnittstelle des optischen Erfassungssystems weitergeleitet und dort zur Codierung verwendet.

[0037] Je nach Eigenschaften der Kryptokarten kann beispielhaft mit etwa 27 Prüfungen pro Sekunde gerechnet werden. Da die Rate der Lesemaschinen bei etwa 10 gelesenen Sendungen pro Sekunde liegt, erscheint es nicht sinnvoll, jeden der AFM-2D-Code-Leser mit einem Krypto-System zu kombinieren. Hinzu kommt, dass auch nicht davon auszugehen ist, dass PC-F-Sendungen zu hundert Prozent auf allen Maschinen gleichzeitig produziert werden. Es erscheint daher sinnvoll, die Krypto-Systeme zu separieren und mehrere PC-F-Leser mit einem Krypto-System zu betreiben. Die Lösung sollte dabei so gewählt sein, dass sie sich skalieren lässt, also mehrere Krypto-Systeme pro Briefzentrum möglich sind. Dies ist zum Beispiel für Briefzentren mit einem hohen Sendungsaufkommen und einer hohen Anzahl Lesemaschinen relevant, bei denen initial ein zweites Krypto-System vorgesehen werden kann. Zudem kann später im Betrieb die Anzahl Server bei entsprechendem Bedarf erhöht werden.

[0038] Die Architektur ist zur Verringerung der Komplexität dabei vorzugsweise so zu wählen, dass die einzelnen Lesemaschinen einem Krypto-System fest zugeordnet und eventuell noch um eine zusätzliche Fallback-Konfiguration erweitert werden, die im Fehlerfalle versucht, auf ein anderes Krypto-System auszuweichen.

[0039] Die Trennung von Krypto-System und AFM-2D-Code-Leser bringt zudem den Vorteil, dass sowohl die Maschinenlesung als auch die Handscannerprüfung mit dem gleichen Krypto-System erfolgen kann, und deshalb die gleiche Funktion nicht doppelt zu implementieren ist, was zusätzlich auch wesentliche Vorteile bei der Implementation der Erfindung bietet.

[0040] Bevorzugte Verfahrensschritte zum Versehen einer Postsendung mit einem digitalen Freimachungsvermerk nach Laden eines Gebührenbetrages von einer zentralen Ladestelle (Postage Point) und Erzeugung des Freimachungsvermerks durch einen lokalen PC sowie anschließender Einlieferung der Postsendung und Überprüfung des auf der Postsendung aufgebrachten Freimachungsvermerks, sind in Fig. 3 dargestellt.

[0041] Unabhängig von der Schlüsselverteilung erfolgt der Ablauf so, dass ein Kunde zuerst einen Portobetrag auf seinen PC lädt. Zur Kennzeichnung der Anfrage wird dabei eine Zufallszahl generiert. Auf der Gebührenbetragsladestelle (Postage Point) wird ein neuer Portobetrag zu dem jeweiligen Kunden erzeugt und aus der übermittelten Zufallszahl, weiteren Informationen zu der Identität des Kundensystems (die Kundensystemidentifikationsangabe, nachfolgend Postage ID genannt) und zu dem Portobetrag wird der sogenannte Cryptostring erstellt, der mit einem auf der Gebührenbetragsladestelle (Postage Point) existierenden geheimen symmetrischen Schlüssel verschlüsselt wird.

[0042] Dieser Cryptostring und der entsprechende Portobetrag werden anschließend auf den Kunden-PC übertragen und zusammen mit der Zufallszahl in dessen "Safe-Box" sicher vor ungewollten Zugriffen abgelegt.

[0043] Wird von dem Kunden im Anschluss an diesen Vorgang mit dem erhaltenen Portobetrag eine Post-Sendung frankiert, so werden die für den 2D-Barcode relevanten Sendungsdaten, unter anderem Cryptostring, Frankierdatum und Frankierbetrag, um die Zufallszahl erweitert und die Postage ID in unverschlüsselter Form gesammelt, und es wird ein Hashwert erstellt, der den Inhalt eindeutig kennzeichnet.

[0044] Da die Zufallszahl in verschlüsselter Form innerhalb des Cryptostrings sowie in unverschlüsselter Form innerhalb des Hashwerts vorliegt, wird sichergestellt, dass die Sendungsdaten nicht verändert, beziehungsweise willkürlich generiert werden können, und es wird ein Rückschluss auf den Ersteller möglich.

[0045] Die relevanten Daten zur Sendung werden dann anschließend in einen 2D-Barcode umgewandelt und als entsprechendes Frankierungskennzeichen durch den Drucker des Kunden auf die Sendung gedruckt. Die fertige Sendung kann daraufhin in den Postkreislauf gegeben werden.

[0046] Bei einer besonders bevorzugten Ausführungsform der Entgeltsicherung wird der 2D-Barcode in dem Briefzentrum von einem AFM-2D-Code-Leser, beziehungsweise von einem Handscanner, gelesen und anschließend geprüft. Die damit verbundenen Prozessschritte werden in der Abbildung unter den Vorgangsnummern 5–8 deutlich. Zur Überprüfung der Korrektheit des 2D-Barcodes übergibt der AFM-2D-Code-Leser die kompletten Sendungsdaten an das Krypto-System. Dort wird eine in den Sendungsdaten enthaltene kryptographische Information, insbesondere des Cryptostrings entschlüsselt, um die bei der Erstellung des Hashwertes verwendete Zufallszahl zu ermitteln.

[0047] Anschließend wird ein Hashwert (auch Message Digest genannt) zu den Sendungsdaten inklusive der entschlüsselten Zufallszahl ermittelt, und es wird überprüft, ob das Ergebnis mit dem im 2D-Barcode enthaltenen Hashwert identisch ist.

[0048] Zusätzlich zu der kryptographischen Validierung erfolgen noch weitere inhaltliche Prüfungen (Vorgangsnummer 7b), die zum Beispiel die doppelte Verwendung eines 2D-Barcodes ausschließen, beziehungsweise prüfen, ob der Kunde durch Betrugsversuche auffällig wurde und deswegen auf einer Negativdatei gelistet ist.

[0049] Das entsprechende Prüfergebnis wird daraufhin an den PC-F-Leser übermittelt, der das Ergebnis an das optische Erfassungssystem (IMM) zur Codierung des Barcodes weiterleitet. Der Barcode wird im Anschluss auf den Brief gespritzt und die Sendungen werden bei einem negativen Prüfergebnis ausgeschleust.

Krypto-System-Architektur

Komponentenübersicht

[0050] Fig. 4 gibt eine Übersicht über die Teilkomponenten des Krypto-Systems, wobei die beschrifteten Pfeile Ein- und Ausgabedatenströme zu externen Systemen darstellen. Da das bevorzugte Entgeltsicherung Zentral-System als Drehscheibe bei der Verteilung der Schlüssel der Gebührenbetragsladestelle (Postage Point) an die Krypto-Systeme der lokalen Entgeltsicherungssysteme verwendet wird und diese Daten zwischengespeichert werden müssen, ist dort jedoch der Validation Controller in der Regel nicht genutzt wird.

[0051] Die Teilkomponenten des Krypto-Systems werden im Folgenden detaillierter beschrieben.

Validation Controller

[0052] Der Validation Controller stellt die Schnittstelle zur Überprüfung des kompletten 2D-Barcodeinhalts dar. Die Überprüfung des 2D-Barcodes besteht aus einer inhaltlichen und einer kryptographischen Überprüfung. Zu diesem Zweck sollte der eingelesene 2D-Barcodeinhalt der Scanner durch den Scanner Controller an den Validation Controller weitergeleitet werden.

[0053] Da sich der verantwortliche Scanner Controller für den drahtgebundenen Scanner und der Validation Controller auf unterschiedlichen Rechnersystemen befinden, ist eine TCP/IP-basierte Kommunikation zwischen ihnen vorzusehen, wobei statt reiner Socket-Programmierung der Einsatz eines darauf aufsetzenden Protokolls Vorteile bietet. Im Rahmen des Krypto-Systems kommen hier der innerhalb der Betriebsdatenerassung (BDE) verwendete Telegrammmanager oder das im Rahmen des optischen Erfassungsystems verwendete Protokoll wie Corba/IIOP in Frage.

[0054] Der Validation Controller initiiert die einzelnen Prüfroutinen, die wiederum ihre Prüfergebnisse an ihn zurückübermitteln.

[0055] Da mehrere AGB-Prüfer mit unterschiedlichen Scannern gleichzeitig tätig werden, ist der Validation Controller "multisessions-fähig" auszulegen. Das heißt, er muss gleichzeitige Prüfanfragen bewerkstelligen und die entsprechende Ausgabe auf den richtigen Scanner lenken können. Zudem sollte er so ausgelegt werden, dass er gleichzeitig mehrere Prüfanfragen, sowie einen Teil der Prüfungsschritte, zum Beispiel Hashwertprüfung und Mindestentgeltprüfung, parallel dazu ausführen kann.

[0056] Zu Beginn einer Sitzung wird dem Controller mitgeteilt, mit welchem Typ von Scanner er kommuniziert, und er bekommt eine Möglichkeit zugeordnet, per CallBack-Methode, Routinen zur Ausgabe und zur manuellen Nachprüfung anzusteuern. Je nach Betriebsart und Scannertyp werden die Ergebnisse dann entweder auf dem Funkscanner oder dem Entgeltsicherung-System ausgegeben, sowie manuelle Prüfergebnisse erfasst.

Krypto Karte

[0057] Eine besondere Problematik liegt in der Aufbewahrung des Schlüssels, mit dem der Cryptostring in einem 2D-Barcode verschlüsselt und zur Prüfung wieder entschlüsselt werden muss. Dieser Schlüssel stellt die Fälschungssicherheit der 2D-Barcodes sicher und deshalb darf es nicht möglich sein, ihn auszuspionieren. Daher muss durch spezielle Sicherheitsmaßnahmen gewährleistet sein, dass dieser Schlüssel niemals im Klartext auf der Festplatte, im Speicher oder bei der Übertragung sichtbar und zudem durch starke kryptographische Verfahren abgesichert ist.

[0058] Rein Software basierte Lösungen bringen hier keine zuverlässige Sicherheit, da an irgendeiner Stelle im System doch ein Schlüssel im Klartext erscheint, oder der Schlüssel mit einem Debugger im Klartext im Speicher ausgelesen werden könnte. Diese Gefahr besteht vor allem auch dadurch, dass die Systeme remote administriert werden können, beziehungsweise zwecks einer Reparatur eventuell außer Haus gegeben werden.

[0059] Zudem erzeugen die kryptographischen Verfahren eine hohe Last auf dem Prozessor des Systems, der im Hinblick auf die durchzuführenden Operationen nicht optimiert ist.

[0060] Es empfiehlt sich daher der Einsatz einer Kryptoprozessorkarte mit folgenden Kennzeichen:

- Spezieller Kryptoprozessor zur Beschleunigung von kryptographischen Verfahren
- Abgeschlossenes Black-Box-System zur Verhinderung des Zugriffs auf sicherheitskritische Daten und Verfahren.

[0061] Bei den Karten, welche diese Kennzeichen erfüllen, handelt es sich um autarke Systeme, die je nach Ausführung über den PCI- oder den ISA-Bus mit dem Rechner verbunden sind und über einen Treiber mit den Softwaresystemen auf dem Rechner kommunizieren.

[0062] Neben batteriegepuffertem Hauptspeicher besitzen die Karten auch einen Flash-Rom-Speicher, in dem ein individueller Anwendungscode gespeichert werden kann. Der direkte Zugriff auf den Hauptspeicher der Karten ist von den äußeren Systemen nicht möglich, wodurch eine sehr hohe Sicherheit gewährleistet ist, da weder die Schlüsseldaten noch die kryptographischen Verfahren zur Bereitstellung der Sicherheit anders als über den gesicherten Treiber greifbar sind.

[0063] Zusätzlich überwachen die Karten mittels eigener Sensoren, ob Manipulationsversuche vorliegen (je nach Kartenausführung, zum Beispiel Temperaturspitzen, Strahlung, Öffnen der Schutzabdeckung, Spannungsspitzen).

[0064] Liegt ein solcher Manipulationsversuch vor, so wird der batteriegepufferte Hauptspeicherinhalt sofort gelöscht und ein Shutdown der Karte durchgeführt.

[0065] Für den Crypto Server sollte die Funktion zur Entschlüsselung der Postage ID, die Funktion zum Prüfen des Hashwertes, sowie die Funktion zum Importieren von Schlüsseldaten direkt auf die Karte geladen werden, da diese Routinen eine hohe Sicherheitsrelevanz besitzen.

[0066] Ferner sollten alle kryptographischen Schlüssel, sowie die Konfigurationen von Zertifikaten, die zur Durchführung der Authentisierung notwendig sind, ebenfalls im batteriegepufferten Speicher der Karte gesichert werden. Verfügt die Karte über nicht genügend Speicher, so existiert auf der Karte in der Regel ein Master Key, mit dem die oben aufgeführten Daten verschlüsselt werden und anschließend auf der Festplatte des Systems abgelegt werden können. Dies erfordert jedoch, dass vor Benutzung dieser Informationen die Daten zunächst wieder entschlüsselt werden.

[0067] Die folgende Tabelle gibt eine Übersicht der in Frage kommenden Kartenmodelle unterschiedlicher Hersteller und nennt gleichzeitig ihre Zertifizierungen.

Kryptokarten für den Einsatz innerhalb des bevorzugten Entgeltsicherungs-Systems für die PC-Frankierung

Hersteller	Typbezeichnung	Zertifizierung
IBM	4758-023	FIPS PUB 140-1 Level 3 und ZKA-eCash
IBM	4758-002	FIPS PUB 140-1 Level 4 und ZKA-eCash (voraus. 07/2000) CCEAL 5 (angestrebt, z.Zt. in Zertifizierungsphase)
Utimaco	KryptoServer	ITSEC-E2 und ZKA-eCash
Utimaco	KryptoServer 2000 (verfügbar ca. 1Q/01)	FIPSPUB 140-1 Level 3, ITSEC-E3 und ZKA-eCash (angestrebt)
Racal/Zaxus	WebSentry PCI	FIPS PUB 140-1 Level 4

[0068] Neben der Erfüllung der an die Karte gestellten Anforderungen ist es wegen der gewünschten Zertifizierung durch das BSI auch sehr wichtig, welche Zertifizierungen die einzelnen Modelle zur Zeit besitzen und welche Zertifizierungen sich zur Zeit im Evaluationsprozess befinden.

[0069] Für die Produkte ausgestellte Zertifikate unterteilen sich dabei in die drei von unterschiedlichen Zertifizierungsstellen vorgenommenen Einstufungen.

[0070] Die ITSEC ist ein von der Europäischen Kommission veröffentlichtes Kriterienwerk zur Zertifizierung von IT-Produkten und IT-Systemen im Hinblick auf deren Sicherheitseigenschaften. Die Vertrauenswürdigkeitsbewertung richtet sich nach den Stufen E0 bis E6, wobei E0 unzureichende und E6 höchste Sicherheit bedeutet. Eine Weiterentwicklung und Harmonisierung mit ähnlichen internationalen Standards sind die CC (Common Criteria), die sich zur Zeit in einem Standardisierungsprozess bei der ISO (ISO Norm 15408) befinden. Dieses Regelwerk wird zur Bewertung der Sicherheit des Systems herangezogen.

[0071] Es gibt zur Zeit noch kein Produkt aus obiger Tabelle, das über ein Zertifikat nach CC verfügt. Das IBM-Modell 4758-002 befindet sich jedoch zur Zeit in einer solchen Zertifizierungsphase.

[0072] Der Standard FIPS PUB 140-1 ist ein von der amerikanischen Regierung herausgegebenes Kriterienwerk zur Beurteilung der Sicherheit von kommerziellen kryptographischen Geräten. Dieses Kriterienwerk orientiert sich sehr stark an Hardwareeigenschaften. Die Bewertung erfolgt in 4 Stufen, bei denen Level 1 die geringste und Level 4 die höchste Sicherheit bedeutet.

[0073] Zusätzlich zu dem oben genannten Bewertungsstandard gibt es ein weiteres Kriterienwerk, das vom Zentralen Kreditausschuss (ZKA) herausgegeben wird und Zulassungen für den Betrieb von IT-Systemen und -Produkten im Bereich electronic cash regelt.

[0074] Neben den bereits erwähnten Eigenschaften der Karten und den zugeteilten Zertifizierungen gibt es jedoch noch eine Reihe weiterer Vorzüge, die nachfolgend kurz aufgelistet sind:

- Erstellung eigener (signierter) Software und Upload auf die Karte möglich
- Integrierter Zufallszahlengenerator (FIPS PUB 140-1 zertifiziert)
- DES, Triple DES und SHA-1 hardwareseitig implementiert
- RSA-Key-Erzeugung und Private/Public Key-Verarbeitung für Schlüssel bis zu 2048 Bit Länge
- Key Management-Funktionen
- Zertifikatsmanagement-Funktionen
- Zum Teil Betrieb mehrerer Kryptokarten parallel in einem System möglich

Krypto Interface

[0075] Die im Rahmen der Kryptokartenapplikation sicherheitsrelevanten Funktionen werden direkt in der Karte gespeichert und sind daher von außen nur über den Kartentreiber zugreifbar. Als Schnittstelle zwischen dem Treiber und dem Validation Controller dient die Krypto Interface-Komponente, welche die Requests für Prüfroutinen per Treiber an die Karte weiterleitet.

[0076] Da mehrere Karten innerhalb eines Rechners zum Einsatz kommen können, liegt die Aufgabe des Krypto Interfaces auch darin, eine Lastverteilung der einzelnen Prüfrequests vorzunehmen. Diese Funktion ist insbesondere dann zweckmäßig, wenn zusätzlich noch einer oder je nach Briefzentrum mehrere AFM-2D-Code-Leser die Prüfroutinen des Krypto-Systems nutzen.

[0077] Eine weitere Aufgabe besteht in der Abwicklung der Kommunikation zwecks Verteilung der Schlüsseldaten. In Stufe 2 existiert eventuell nur ein rudimentärer Mechanismus, der die zur Sicherheit verschlüsselten Schlüssel innerhalb

einer signierten Datei überträgt. Eine Anforderung an das Krypto Interface liegt dann darin, ein Utility bereitzustellen, das den Import einer solchen Datei ermöglicht.

Funktionen des Krypto-Systems

Ablauf der Prüfung im Validation Controller

[0078] Zur Prüfung des 2D-Barcodes wird von dem Validation Controller eine zentrale Prüffunktion als Schnittstelle zu den Scanner- beziehungsweise den Lesesystemen zur Verfügung gestellt. Diese Prüffunktion koordiniert den Ablauf der einzelnen Teilprüfungen.

[0079] Die aus den einzelnen Teil-Prüfroutinen übermittelten Codes für den Entgeltsicherung-Vorfall werden anhand einer vordefinierten Tabelle, die vorzugsweise zentral gepflegt und auf das Krypto-System übertragen wird, in den entsprechenden Entgeltsicherungs-Code umgewandelt. Innerhalb dieser Tabelle werden zusätzlich Prioritäten festgelegt, die regeln welcher Entgeltsicherungs-Code zugewiesen wird, wenn mehrere Entgeltsicherungs-Vorfälle erkannt wurden.

[0080] Dieser Entgeltsicherungs-Code wird anschließend zusammen mit einem beschreibenden Text als Prüfergebnis zurückgeliefert. Je nach weiterverarbeitendem System außerhalb des Krypto Systems wird dieses Ergebnis dann auf dem Funkscanner oder innerhalb der Entgeltsicherung-Anwendung ausgegeben, beziehungsweise bei der automatischen Prüfung in einen TTT2-Code umgewandelt und die Sendung damit bedruckt.

[0081] Da die Abläufe zwischen den Handscannersystemen und den automatischen Lesesystemen unterschiedlich sind, wird für beide Anwendungsfälle eine unterschiedliche Funktion implementiert.

[0082] Je nachdem, welcher Kommunikationsmechanismus zwischen dem Lesesystem und dem Validation Controller verwendet wird, unterscheidet sich der Aufruf und die Rückgabe der Ergebnisse. Im Falle des Einsatzes eines synchronen RPC-basierten Protokolls wie Corba/IIOP wird die Prüfmethode direkt aufgerufen und die Prüfergebnisse werden nach Abschluss der Prüfung übergeben. Der Client, also der ScannerController, beziehungsweise das Lesesystem warten in diesem Fall auf die Ausführung und die Rückgabe der Prüfergebnisse. Bei letzterem ist daher auf dem Client ein Threadpool vorzusehen, der die parallele Prüfung mehrerer Anfragen durchführen kann.

[0083] Bei dem asynchronen Mechanismus mittels TGM wird vom Scanner Controller, beziehungsweise dem Lesesystem, die Prüfmethode nicht direkt aufgerufen, sondern es wird ein Telegramm an das Krypto-System gesendet, welches die Prüfanforderung, den Inhalt des 2D-Barcodes und weitere Informationen wie aktuelles Sortierprogramm enthält. Bei Eingang dieses Telegramms auf dem Krypto-System wird die Prüffunktion aufgerufen, durchgeführt und die Lese- und Prüfergebnisse wiederum als ein neues Telegramm zurückgesendet. Der Vorteil bei diesem Verfahren liegt darin, dass auf dem anfordernden System der Prozess nicht blockiert wird, bis das Ergebnis vorliegt.

Prüfung für Handscannersysteme

[0084] Die Prüfroutine für die Handscannersysteme erwartet als Eingabewerte die Session-ID sowie den Inhalt des 2D-Barcodes. Als zusätzlicher Parameter wird auch noch die ID des Sortierprogramms erwartet. Der zuletzt genannte Parameter dient zur Bestimmung des Mindestentgelts.

[0085] Fig. 5 zeigt eine Übersicht über den Ablauf der Prüfung innerhalb des Validation Controllers für den Fall, dass diese von einem Handscannersystem ausgelöst wurde. Es wird dabei von einer Prüfung mit einem Funkscanner mit anschließendem manuellen Vergleich der Anschrift mit dem 2D-Barcodeinhalt ausgegangen. Bei einem drahtgebundenen Scanner würde die Darstellung analog auf dem Entgeltsicherung-System, beziehungsweise der Entgeltsicherung-Anwendung erfolgen.

[0086] Ein bevorzugter Überprüfungsablauf durch Einsatz eines Funkscanners, eines Scanner-Controllers und einer Überprüfungseinheit (Validation Controller) ist in Fig. 5 dargestellt.

[0087] Die Überprüfungseinheit steuert bei dem dargestellten, besonders bevorzugten Ausführungsbeispiel, einen Ablauf von Teilprüfungen, wobei die erste Teilprüfung ein Einlesen eines in dem digitalen Freimachungsvermerks enthaltenen Matrixcodes beinhaltet. Der eingelesene Matrixcode wird zunächst von einem Funkscanner an einen Scanner-Controller übertragen. Anschließend erfolgt in dem Bereich des Scanner-Controllers eine Prüfung des Matrixcodes sowie eine Übermittlung an die Überprüfungseinheit. Die Überprüfungseinheit steuert eine Aufspaltung des Codeinhalts. Das Leseergebnis wird anschließend an die Erfassungseinheit – im dargestellten Fall ein Funkscanner – übermittelt. Hierdurch erfährt beispielsweise ein Benutzer der Leseeinheit, dass es möglich war, den Freimachungsvermerk zu lesen und die in der Matrix enthaltenen Informationen dabei zu erkennen. Anschließend entschlüsselt die Überprüfungseinheit einen in dem Matrixcode enthaltenen Cryptostring. Hierzu wird vorzugsweise zunächst die Version des voraussichtlich für die Erstellung des Freimachungsvermerks eingesetzten Schlüssels überprüft. Anschließend wird der in dem Cryptostring enthaltene Hashwert geprüft.

[0088] Ferner erfolgt eine Prüfung des vorgesehenen Mindestentgelts.

[0089] Außerdem wird eine Identifikationsnummer (Postage ID) des die Erzeugung des Freimachungsvermerks steuernden Kundensystems überprüft.

[0090] Hieran anschließend erfolgt ein Abgleich der Identifikationsnummer mit einer Negativliste.

[0091] Durch diese Überprüfungsschritte ist es in dieser besonders einfachen und zweckmäßigen Form möglich, auf einfache Weise unberechtigt erzeugte Freimachungsvermerke zu ermitteln.

[0092] Das Ergebnis der Übermittlung wird als eine digitale Nachricht übermittelt, wobei die digitale Nachricht beispielsweise an den ursprünglichen Funkscanner übermittelt werden kann. Hierdurch kann beispielsweise ein Benutzer des Funkscanners die Sendung aus dem Sendungslauf ausschleusen. Bei einer automatisierten Durchführung dieser Verfahrensvariante ist es jedoch selbstverständlich gleichermaßen möglich, die Sendung aus dem normalen Verarbeitungslauf der Postsendungen auszuschleusen.

[0093] Vorzugsweise wird das Ergebnis der Prüfung im Bereich der Überprüfungseinheit protokolliert.

[0094] Als Rückgabewert sollte der zu dem Entgeltsicherung-Vorfall gehörende Code und die zugehörige Textmeldung sowie das 2D-Barcode-Objekt zurückgegeben werden.

Prüfungsablauf beim AFM-2D-Code-Leser

[0095] Als Eingabeparameter der Prüfroutine für den AFM-2D-Code-Leser wird ebenfalls die Session-ID, sowie der Inhalt des 2D-Barcodes und die eindeutige Kennzeichnung des zur Zeit aktiven Sortierprogramms erwartet.

[0096] Fig. 6 zeigt eine Übersicht über den Ablauf der Prüfung innerhalb des Validation Controllers für den Fall, dass diese von einem Lesesystem ausgelöst wurde.

[0097] In der Abbildung sind zur Verdeutlichung des Ablaufs auch zusätzlich das optische Erfassungssystem (IMM-System) sowie der AFM-2D-Code-Leser aufgeführt, um den Gesamtkontext der Prüfung darzustellen. Der Anteil des Krypto-Systems beschränkt sich allerdings darauf, die Funktionen zwischen 2D-Barcode und der Rückgabe sowie der Protokollierung des Ergebnisses zu prüfen.

[0098] Im Falle der Telegrammmanager-Schnittstelle würden auf dem Validation Controller mehrere Service Tasks gestartet, die auf Prüfanforderungstelegramme warten und mit dem Telegramminhalt die Prüfroutine aufrufen würden. Das Ergebnis der Prüfroutine wird abgewartet und in ein Telegramm verpackt und an den Anforderungsclient zurückgesendet.

[0099] In Fig. 6 ist eine weitere bevorzugte Ausführungsform einer Steuerung eines Ablaufs von Teilprüfungen durch die Überprüfungseinheit (Validation Controller) dargestellt. Bei dieser weiteren bevorzugten Ausführungsform erfolgt eine Erfassung der Freimachungsvermerke durch ein automatisches optisches Erkennungssystem (Prima/IMM). Die Daten werden von der optischen Überprüfungseinheit zu einer Lese- und Erfassungseinheit (AFM-2D-Code-Leser).

[0100] Bei der in Fig. 6 dargestellten Ausführungsform des Verfahrens zum Überprüfen der Gültigkeit von digitalen Freimachungsvermerken erfolgt ein Einlesen der digitalen Freimachungsvermerke vorzugsweise in einer noch stärker automatisierten Weise, beispielsweise durch optische Erfassung einer Stelle einer Postsendung, auf der vorzugsweise ein Freimachungsvermerk angeordnet ist. Die weiteren Überprüfungsschritte erfolgen im Wesentlichen entsprechend des anhand von Fig. 5 dargestellten Prüfungsablaufs.

[0101] Der Rückgabewert der Prüfroutine besteht einerseits aus dem Entgeltsicherung-Code und einer zugehörigen Meldung sowie dem umgewandelten und um die Postage ID erweiterten Inhalt. Aus diesen Rückgabewerten wird ein Telegramm erzeugt und an das anfordernde Lesesystem übermittelt.

Inhaltliche Prüfungen

2D-Barcodeinhalt aufspalten und umformen
Input: gescannter 2D-Barcode

Beschreibung

[0102] In dieser Funktion ist der aus 80 Bytes bestehende Inhalt des 2D-Barcodes aufzuteilen und in ein strukturiertes Objekt, im Folgenden mit 2D-Barcode-Objekt bezeichnet, umzuwandeln, um eine bessere Darstellungsmöglichkeit sowie eine effizientere Nachbearbeitung zu erreichen. Die einzelnen Felder und Umwandlungen sind in der nachfolgenden Tabelle beschrieben:

Bei der Umwandlung der Binär- in Dezimalzahlen ist darauf zu achten, dass das linke Byte einer Bytefolge das höchstwertige Byte ist. Kann eine Umwandlung eventuell wegen eines Typenkonflikts oder fehlender Daten nicht erfolgen, so ist eine Entgeltsicherungs-Vorfallsmeldung "PC-F-Barcode nicht lesbar" zu generieren und an den Validation Controller zurückzugeben. Eine weitere inhaltliche, beziehungsweise kryptographische Überprüfung ist in diesem Fall nicht sinnvoll.

Feld	Typ	umzuwandeln in	Beschreibung
Post-Unternehmen	ASCII (3 Byte)		keine Umwandlung notwendig
Frankierart	Binär (1 Byte)	Smallinteger	
Versionskennzeichen	Binär (1 Byte)	Smallinteger	Versionsnummer des Verfahrens
Key-Nr.	Binär (1 Byte)	Smallinteger	Schlüsseltyp
CryptoString	Binär (32 Byte)		Bytefolge ist unverändert zu übernehmen, nach Entschlüsselung wird die PostageID herausgespalten
PostageID		Text(16 Zeichen)	Wird nach Entschlüsselung des Cryptostring gefüllt
laufende Sendungsnummer	Binär (3 Byte)	Integer	nur positive Zahlen
Produktschlüssel	Binär (2 Byte)	Integer	positive Zahlen, Verweis auf zugehörige Referenztabelle
Entgelt	Binär (2 Byte)	Float	Umwandlung in positive Dezimalzahl, die

			durch hundert zu teilen ist, Angabe in Euro
Frankierdatum	Binär (3 Byte)	Date	Nach Umwandlung in positive Dezimalzahl, lässt sich das Datum nach dem Format YYYYMMDD umwandeln
EmpfängerPLZ	Binär (3 Byte)	2 Werte, einen für Land, einen für PLZ-Code	Nach Umwandlung in positive Dezimalzahl ergeben die ersten beiden Ziffern den Ländercode, die fünf restlichen Ziffern die PLZ
Straße/Postfach	ASCII (6 Byte)	Straßenkürzel oder Postfach	Handelt es sich bei den ersten Ziffern um Zahlen, dann ist eine PLZ codiert, ansonsten die ersten und letzten drei Stellen der Straße mit Hausnummer
Portorestbetrag	Binär (3 Byte)	Float + Währungsfeld (Text 32 Zeichen)	Nach Umwandlung in eine positive Dezimalzahl ergibt die erste Ziffer die Währung (1=Euro), die nachfolgenden vier Ziffern die Vorkomma- und die restlichen zwei Ziffern die Nachkommastellen
Hash-Wert	Binär (20 Byte)		Bytefolge ist unverändert zu übernehmen, dient zur kryptographischen Validierung der Frankierung

Returnwert: 2D-Barcode-Objekt Warnungscode 00 falls Umwandlung OK, ansonsten Warnung für Entgeltsicherungs-Vorfall "PC-F-Barcode nicht lesbar"

Versionsnummernprüfung

Input: aktuelles 2D-Barcode-Objekt

Beschreibung

[0103] Aus den ersten drei Feldern lässt sich die Version des 2D-Barcodes erkennen. Hieraus wird auch ersichtlich, ob es sich bei dem Frankiervermerk überhaupt um einen 2D-Barcode der Deutschen Post und nicht um einen 2D-Barcode eines anderen Dienstleisters handelt. Die Feldinhalte sind mit einer in der Anwendung vorkonfigurierten Liste gültiger Werte zu vergleichen. Wird keine Übereinstimmung gefunden, so wird eine Entgeltsicherungs-Warnung "PC-F-Version" zurückgeliefert. Die Überprüfung weiterer inhaltlicher als auch kryptographischer Aspekte ist dann sinnlos und sollte nicht weiterverfolgt werden.
Returnwert: Warnungscode 00 falls Versionsprüfung OK, ansonsten Warnungscode für Entgeltsicherung-Vorfall "PC-F-Version"

Postage ID überprüfen

Input: 2D-Barcode-Objekt mit entschlüsselter Postage ID

Beschreibung

[0104] Die in dem 2D-Barcode enthaltene Postage ID ist durch ein Prüfziffernverfahren (CRC 16) abgesichert, das an dieser Stelle zu überprüfen ist. Sollte diese Überprüfung fehlschlagen, so ist als Ergebnis eine Entgeltsicherung-Warnung "PC-F Fälschungsverdacht (Postage ID)" zurückzugeben. Zur Überprüfung der Postage ID ist die vorherige Entschlüsselung des CryptoStrings erforderlich.
Returnwert: Code "00" falls Prüfung OK, ansonsten Warnungscode für Entgeltsicherung-Vorfall "PC-F Fälschungsverdacht (Postage ID)"

Prüfung der Zeitüberschreitung

Input: 2D-Barcode-Objekt

Beschreibung

[0105] Diese Funktion dient der automatischen Überprüfung des Zeitintervalls zwischen Frankierung einer PC-freigemachten Sendung und deren Verarbeitung auf dem Briefzentrum. Zwischen beiden Daten darf nur eine bestimmte Anzahl von Tagen liegen. Die Anzahl der Tage richtet sich dabei nach dem Produkt und dessen Laufzeiten plus einem Karenztag.
[0106] Die Konfiguration des Zeitraums wird vorzugsweise in einer Produkt-Gültigkeitszeitraum-Relation gespeichert und im Rahmen einer Pflegemaske zentral gepflegt. In der Relation werden zu jedem für PC-Frankierung möglichen Produktschlüssel (Feld des 2D-Barcodes) die zugehörige Anzahl Tage, die zwischen Frankierung und Verarbeitung auf dem Briefzentrum liegen dürfen, festgehalten. In einem vereinfachten Verfahren wird nur eine Zeitraumangabe vorkonfiguriert, die sich auf Standardsendungen bezieht und als Konstante im System hinterlegt wird.
[0107] Zur Überprüfung wird die Anzahl der Tage zwischen dem aktuellen Testdatum bei der Verarbeitung und dem im 2D-Barcode enthaltenen Datum gebildet, zum Beispiel 02.08. bis 01.08. = 1 Tag. Ist die ermittelte Anzahl Tage größer als der für das Produkt vorgegebene Wert, so wird der dem Warnungsfall "PC-F-Datum (Frankierung)" zugeordnete Entgeltsicherungs-Code an den Validation Controller zurückgegeben, anderenfalls ein Code, der die erfolgreiche Prüfung dokumentiert. Wenn in einem vereinfachten Verfahren immer mit dem Wert für Standardsendungen verglichen wird, sollte nach Ausgabe des Prüfergebnisses die Möglichkeit gegeben sein, beispielsweise manuell über eine Taste am Scanner, dieses Prüfergebnis zu korrigieren, falls das aktuelle Produkt eine längere Laufzeit zulässt.
[0108] Eine weitere Prüfung der Zeitüberschreitung bezieht sich auf den Inhalt der Postage ID. Der im Rahmen einer Vorgabe heruntergeladene Portobetrag und damit auch die Postage ID besitzen einen vorgegebenen Gültigkeitszeitraum, in welchem die Sendungen zu frankieren sind. In der Postage ID ist der Zeitpunkt enthalten, bis zu welchem der Portobetrag gültig ist. Ist das Frankierdatum um eine bestimmte Anzahl Tage größer als dieses Gültigkeitsdatum, so wird der zur Entgeltsicherung-Warnung "PC-F-Datum (Portobetrag)" gehörende Entgeltsicherungs-Warnungscode zurückgegeben.
Returnwert: Code "00" falls Prüfung OK, ansonsten Warnungscode für Entgeltsicherung-Vorfall "PC-F-Datum (Portobetrag)" oder "PC-F-Datum (Frankierung)"

Entgeltprüfung

Input: 2D-Barcode-Objekt; aktuelle Sortierprogramm-ID

Beschreibung

[0109] Innerhalb dieser Funktion erfolgt die Prüfung des im 2D-Barcode enthaltenen Entgeltes gegen ein Mindestentgelt, das für Sendungen des zugehörigen Sortierprogramms definiert ist. Bei den Beträgen handelt es sich um Euro-Beträge.
[0110] Die Zuordnungen werden zwischen Sortierprogramm und Mindestentgelt über eine automatische Schnittstelle geliefert.
[0111] Ein vereinfachtes Verfahren ist ähnlich wie bei der Prüfung der Zeitüberschreitung anzuwenden. Hier wird in der Konfigurationsdatei zu der Anwendung ein konstantes Mindestentgelt definiert, das für alle Sendungen gilt. Daher ist die Übergabe des Sortierprogramms nicht erforderlich.
[0112] Bei der anschließenden Prüfung wird verglichen, ob das im 2D-Barcode enthaltene Mindestentgelt unterhalb dieser Marke liegt. Ist dies der Fall, so wird der dem Entgeltsicherungs-Vorfall "PC-F Unterfrankierung" zugeordnete Code zurückgegeben, ansonsten der Erfolgscode.
Returnwert: Code "00" falls Prüfung OK, ansonsten Warnungscode für Entgeltsicherung-Vorfall "PC-F-Unterfrankierung"

Abgleich mit Negativdatei

Input: 2D-Barcode-Objekt mit entschlüsselter Postage ID

Beschreibung

[0113] Innerhalb dieser Funktion erfolgt die Prüfung, ob die zu dem 2D-Barcode gehörende Postage ID in einer Nega-

tivdatei enthalten ist. Die Negativdateien dienen dazu, Sendungen von Kunden, die durch Missbrauchsversuche aufgefallen sind, beziehungsweise deren PC entwendet wurde, aus dem Beförderungslauf herauszunehmen.

[0114] Die Negativdateien werden dabei zentral im Rahmen des Projektes Datenbank Freimachung gepflegt. Im Rahmen der Schnittstelle zu diesem Projekt ist das Verfahren für den Austausch der Daten auf die dezentralen Briefzentrum-Systeme zu bestimmen.

[0115] Wenn die Pflegeanwendung, beziehungsweise der Datenaustausch eventuell noch nicht existiert, ist hier ein Übergangsmechanismus zu schaffen. Die Pflege dieser Daten könnte übergangsweise in einem Excel-Sheet erfolgen, aus dem eine csv-Datei generiert wird. Diese Datei sollte per eMail an die AGB-Prüfer verschickt und von diesen über einen vorzusehenden Importmechanismus in den Systemen eingelesen werden. Später erfolgt die Übertragung dann über den innerhalb des bevorzugten Entgeltsicherungs-IT-Feinkonzeptes definierten Weg.

[0116] Eine Postage ID kennzeichnet eine einzelne Vorgabe, die ein Kunde von dem System (Postage Point) abruft. Diese Vorgaben werden in einer sogenannten Safebox auf dem Kundensystem gespeichert. Es handelt sich hierbei um eine Hardwarekomponente in Form einer SmartCard inklusive Lesesystem, beziehungsweise eines Dongles. In der Safebox werden die Vorgabebeträge sicher aufbewahrt und der Kunde kann davon einzelne Frankierungsbeträge abrufen, ohne online mit der Gebührenbetragsladestelle (Postage Point) verbunden zu sein.

[0117] Jede Safe Box ist durch eine eindeutige ID gekennzeichnet. Diese Safebox-ID wird in der Negativdatei eingetragen, falls die zugehörigen Sendungen wegen Missbrauchsverdacht ausgeschleust werden sollen. Die Safebox-ID ist aus mehreren Feldern zusammengesetzt. Neben dem eindeutigen Schlüssel sind in der Safebox-ID auch weitere Felder wie Gültigkeitsdatum und Prüfziffer enthalten. Zur eindeutigen Identifizierung der Safebox sind die ersten drei Felder der Safebox-ID maßgeblich. Diese finden sich auch in den ersten drei Feldern der PostageID wieder, wodurch die Zuordnung zwischen Safebox und Vorgabe erfolgen kann. Die Felder sind in der nachfolgenden Tabelle beschrieben:

Byte Nr.	Länge	Bedeutung	Dateninhalt	Kommentar
b1	1	Anbieter-Kennzeichnung	00	nicht benutzt
			01	Test-Anbieter: Postversand-unternehmen
			FF	Postage-Point-Box des Postversand-unternehmens
b2	1	Zugelassene Modell-Nr.	XX	Für jeden Hersteller von 01 (erstes eingereichtes Modell) aufsteigend für jedes neu zugelassene Modell zu belegen.
b3, b4, b5	3	Seriennummer des Modells	XX XX XX	Für jedes zugelassene Modell jedes Herstellers von 00 00 01 bis FF FF FF aufsteigend zu belegen.

[0118] Sind die ersten drei Felder der Postage ID der aktuell geprüften Frankierung identisch mit den ersten drei Feldern einer in der Negativdatei enthaltenen Safebox-ID, so wird der innerhalb der Negativdatei dem Kunden zugeordnete Entgeltsicherung-Vorfall zurückgegeben, ansonsten der Erfolgscode.

Returnwert: Code "00" falls Prüfung OK, ansonsten dem Kunden, beziehungsweise der Safe-Box in der Negativdatei zugeordneter Warnungscode

Vergleich 2D-Barcodeinhalt mit Sendungsklartext

Input: 2D-Barcode-Objekt

Beschreibung

[0119] Um zu verhindern, dass Kopien von 2D-Barcodes erstellt werden können, wird ein Vergleich zwischen den im 2D-Barcode kodierten Sendungsdaten und den auf dem Brief im Klartext angegebenen Daten durchgeführt. Dieser Vergleich ist bei den Funkscannern direkt möglich, da dort ausreichende Darstellungs- und Eingabemöglichkeiten vorhanden sind. Bei den Handscannern mit Drahtanbindung ist die Prüfung auf dem PC (Entgeltsicherung-System) vorzunehmen.

[0120] Der Ablauf sieht so aus, dass der Validation Controller nach Ablauf der automatisierten Prüfungen die Ausgabe der Daten des 2D-Barcodes auf dem Funkscanner, beziehungsweise auf dem Entgeltsicherungs-PC, veranlasst. Hierzu

steht ihm eine Callback-Methode zur Verfügung, die am Anfang einer Sitzung zugeordnet wird.

[0121] Diese ruft er mit dem aktuellen 2D-Barcode-Objekt auf. Daraufhin sind der Scanner Controller, beziehungsweise der Entgeltsicherung-PC für die Darstellung des 2D-Barcodeinhalts verantwortlich und liefern als Returnwert (nach Bearbeitung durch den Prüfer) der Callback-Methode eine "00", beziehungsweise einen zugehörigen Fehlercode zurück.

[0122] Bei erfolgreicher Auswertung wird der Erfolgscode, ansonsten der Code der Entgeltsicherungs-Warnung "PC-F-Klartext" zurückgegeben.

[0123] Bei einer automatischen Prüfung ist diese Prüfung nicht erforderlich. Hier kann die Prüfung vorzugsweise im Rahmen der zentralen Auswertungen offline entweder mittels Umsatzvergleichen oder über einen Vergleich der Zielpostleitzahl mit der im 2D-Barcode enthaltenen Postleitzahl erfolgen.

Returnwert: Code "00" falls Prüfung OK, ansonsten Warnungscode für Entgeltsicherung-Vorfall "PC-F-Klartext"

Kryptographische Prüfungen

[0124] Die kryptographische Prüfung besteht aus zwei Teilen:

a) der Entschlüsselung des Cryptostrings und
b) dem Hashwert-Vergleich.

[0125] Beide Verfahren sind in dem geschützten Bereich der Kryptokarte durchzuführen, da ein Kunde bei Ausspionage der bei der Verarbeitung anfallenden Information, gültige Frankierungshashwerte erzeugen könnte.

Cryptostring entschlüsseln

Input: 2D-Barcode-Objekt

Beschreibung

[0126] Als Eingangsparameter erhält diese Funktion das aufgesplittete 2D-Barcode-Objekt des Scanergebnisses. Es wird anhand des Frankierungsdatums und der Key-Nummer der für diesen Zeitpunkt gültige symmetrische Schlüssel herausgesucht und der CryptoString des übergebenen Objektes mit Hilfe dieses Schlüssels nach dem Verfahren Triple DES CBC entschlüsselt. Mit welchem Wert der Initialisierungsvektor vorzubelegen ist, beziehungsweise ob mit Inner- oder Outerbound-CBC und mit welcher Blocklänge gearbeitet wird, wird im Rahmen der Schnittstelle zu dem Entgeltsicherungssystem entschieden.

[0127] Sollte der in dem 2D-Barcode enthaltene Schlüssel auf dem Kryptosystem nicht vorhanden sein, so wird die Entgeltsicherung-Warnung "PC-F Fälschungsverdacht (Schlüssel)" mit der Fehlermeldung, dass der Schlüssel mit der Key-Nummer nicht gefunden wurde, zurückgegeben.

[0128] Das Ergebnis der Operation besteht aus der entschlüsselten Postage ID, sowie der entschlüsselten Zufallszahl. Die entschlüsselte Postage ID wird in einem entsprechenden Feld des 2D-Barcode-Objektes eingetragen. Die Zufallszahl sollte aus Sicherheitsgründen nicht bekannt gemacht werden, da der Kunde bei Besitz dieser Information gültige Hashwerte erzeugen und damit 2D-Barcodes fälschen könnte.

[0129] Im Anschluss an die Entschlüsselung wird aus der Methode heraus die Hashwertberechnung aufgerufen und deren Rückgabewert zurückgegeben.

Hashwertberechnung

Input: 2D-Barcode-Objekt entschlüsselte Zufallszahl aus dem Cryptostring (die entschlüsselte Zufallszahl darf nicht außerhalb der Karte bekannt sein)

Beschreibung

[0130] Die Funktion der Hashwertberechnung ermittelt aus den im 2D-Barcode-Objekt enthaltenen Original-Scanergebnis die ersten 60 Bytes. Daran werden die entschlüsselte Postage ID, sowie die übergebene entschlüsselte Zufallszahl angehängt. Hieraus wird nach dem Verfahren SHA 1 ein Hashwert berechnet und mit dem im 2D-Barcode-Objekt enthaltenen Hashwert des 2D-Barcodes verglichen. Stimmen alle 20 Bytes überein, so ist die kryptographische Überprüfung erfolgreich, und es wird ein entsprechender Rückgabewert zurückgeliefert.

[0131] Bei Nichtübereinstimmung wird eine Entgeltsicherung-Warnung "PC-F-Fälschungsverdacht (Hashwert)" an den Validation Controller zurückgegeben.

[0132] Als Rückgabewert wird zusätzlich der errechnete Hashwert übermittelt, damit dieser bei dem Prüfergebnis mit ausgegeben werden kann.

Returnwert: errechneter Hashwert Code "00" falls Prüfung OK, ansonsten Warnungscode für Entgeltsicherung-Vorfall
"PC-F-Fälschungsverdacht (Hashwert)" oder
"PC-F-Fälschungsverdacht (Schlüssel)"

Ergebnisausgabe

Prüf- und Leseergebnis darstellen

Beschreibung

[0133] Über eine Callback-Methode hat der Validation Controller die Möglichkeit, eine Ergebnisausgabe auf dem zur aktuellen Prüfung gehörenden Ausgabegerät anzusteuern. Hierzu übergibt er dieser Callback-Methode das 2D-Barcode-Objekt und den ermittelten Entgeltsicherung-Warnungscode. Als Rückgabewert kann der Code des von dem AGB-Prüfer ausgewählten Nachbearbeitungsverfahrens geliefert werden.

[0134] Die Callback-Methode für die Ausgabe wird, ebenfalls zu Beginn der Session, bei der Anmeldung am Validation Controller zugewiesen.

Ergebnisprotokollierung

Input: 2D-Barcode-Objekt, Code des Prüfergebnisses

Beschreibung

[0135] Die Ergebnisprotokollierung erfolgt in einem vereinfachten Verfahren in einer Datei auf dem System, auf dem der Validation Controller läuft. In der Regel werden die Ergebnisse, beziehungsweise Berichtigungssätze direkt an BDE übermittelt und über die bevorzugte Entgeltsicherungs-BDE-Schnittstelle in die Datenbank des bevorzugten lokalen Entgeltsicherungs-Systems geschrieben.

[0136] Vorzugsweise werden die Postage ID, die fortlaufende Nummer, das Frankierdatum, das Entgelt, der Produktschlüssel, die PLZ, der Entgeltsicherungs-Ergebniscode, der Meldungstext, die Dauer der Prüfung, der Zeitpunkt der Prüfung, die ID des Scanners, die Betriebsart des Scanners, der Erfassungsmodus, sowie die Weiterverarbeitungsart gespeichert. Alle Werte werden durch ein Semikolon voneinander getrennt in jeweils einem Satz pro Sendung ausgegeben und sind so zum Beispiel in Excel weiter auswertbar.

[0137] Befindet sich das System in der Betriebsart "Ersterfassung", so ist in der Spalte Erfassungsmodus ein "e", ansonsten ein "n" für Nacherfassung einzugeben.

Stammdatenbereitstellung

Beschreibung

[0138] Für die inhaltliche Überprüfung sind eine Reihe von Stammdaten notwendig. Es handelt sich hierbei um:

- PC-F-Negativdatei
- Sortierprogramme und Mindestentgelte
- Allgemeines Mindestentgelt
- Produktschlüssel PC-F
- Maximale Einlieferungszeit je Produktschlüssel PC-F
- Allgemeine maximale Einlieferungszeit
- Entgeltsicherung-Vorfälle, Prioritäten und Zuordnung zu Weiterbehandlungsanweisungen
- Weiterbehandlungsanweisungen

[0139] Stammdaten können in einer Übergangszeit mit Ausnahme der PC-F-Negativdatei sowie der kryptographischen Schlüssel der Gebührenbetragsladestelle (Poltage Point) fest vorkonfiguriert werden.

[0140] Falls notwendig, können für einen Teil der Daten einfache Bearbeitungs- und Verteilanwendungen implementiert werden. Die Pflege sollte dann in einem Excel-Sheet erfolgen, aus dem eine csv-Datei generiert wird. Diese Datei sollte per eMail an die AGB-Prüfer verschickt und von diesen über einen vorzusehenden Mechanismus in den Systemen eingelesen werden.

[0141] In der Regel werden die Daten entsprechend dem im Bevorzugte Entgeltsicherung-IT-Feinkonzept beschriebenen Verfahren verteilt, beziehungsweise ein Zugriff auf diese Daten ermöglicht.

[0142] Die zugehörigen Datenstrukturen werden im Datenmodell zum Feinkonzept Bevorzugte Entgeltsicherung beschrieben.

Verteilung der Schlüsseldaten

[0143] Die symmetrischen Schlüssel, die auf der Gebührenbetragsladestelle (Poltage Point) zur Absicherung der 2D-Barcodeinhalte dienen und welche das Krypto-System zur Validierung benötigt, werden aus Sicherheitsgründen in regelmäßigen Abständen ausgetauscht. Bei Einsatz in allen Briefzentren müssen die Schlüssel vom (Postage Point) zu den Krypto-Systemen automatisch und sicher übertragen werden.

[0144] Der Austausch sollte dabei über den bevorzugten Entgeltsicherungs-Server erfolgen, da bei der Gebührenbetragsladestelle (Postage Point) nicht konfiguriert werden sollte, welche bevorzugten lokalen Entgeltsicherungs-Systeme und welche Krypto-Systeme dazu existieren.

[0145] Besonders bevorzugte Verfahrensschritte für einen Austausch von Schlüsseln sind in Fig. 7 dargestellt. Der bevorzugte Schlüsselaustausch erfolgt zwischen einer zentralen Ladestelle (Postage Point), einem zentralen Crypto Server und mehreren lokalen Crypto Servern.

[0146] Da die symmetrischen Schlüssel von großer Bedeutung für die Fälschungssicherheit der 2D-Barcodes sind, muss der Austausch durch starke Kryptographie und durch eindeutige Authentisierung der Kommunikationspartner abgesichert sein.

Konfiguration

Grundkonfiguration/Key Management der Crypto Hardware

[0147] Für die Grundkonfiguration der Kryptokarte sind verschiedene Maßnahmen notwendig. Sie sollten durch einen Sicherheitsadministator durchgeführt werden. Es handelt sich dabei grob um folgende Tätigkeiten:

- Installation des Software-APIs auf der Karte
- Generierung, beziehungsweise Installation der privaten Schlüssel zur Absicherung von Administrationsanwendungen und einzuspielender Software

[0148] Je nach ausgewähltem Kartentyp und -hersteller sind dabei unterschiedliche Maßnahmen notwendig.

[0149] Die für das bevorzugte Entgeltsicherungs-System vorgesehene anwendungsbezogene Grundkonfiguration der Kryptokarte besteht aus folgenden Schritten:

- Sichere Verschlüsselung und Übertragung der symmetrischen Schlüssel auf die Karte – beispielsweise RSA-Schlüsselpaar – bei gleichzeitiger Zertifikatserzeugung für den Public Key und Ausgabe des Keys
- Zertifikat der Gebührenbetragsladestelle (Postage Point) fest vorkonfigurieren zur Sicherstellung, dass der zu importierende Schlüssel von der Gebührenbetragsladestelle (Postage Point) ausgestellt wurde.

Grundkonfiguration der Krypto-System-Applikation

[0150] Jeder Scanner, jeder Benutzer und jede Kryptokarte innerhalb des Krypto-Systems muss durch eine eindeutige ID gekennzeichnet sein. Letztlich ist auch jeder AFM-2D-Code-Leser durch eine eindeutige ID zu identifizieren.

Login/Logoff

[0151] Zu Beginn einer Session mit dem Validation Controller muss ein Login erfolgen. Dieses Login enthält als Parameter die Scanner-ID, die User ID, sowie die Callback-Methoden für die manuelle Prüfung, beziehungsweise die Ausgabe der Lese- und Prüfergebnisse.

[0152] Als Rückgabewert wird eine Session-ID zurückgeliefert, die bei folgenden Prüfungsaufrufen innerhalb der Sitzung mit zu übergeben ist. Zu der Session ID wird auf dem Validation Controller ein Session Context gespeichert, in dem die Übergabeparameter gespeichert sind.

[0153] Nimmt der Benutzer während seiner Sitzung Änderungen an der Betriebsart, an dem vordefinierten Produkt, beziehungsweise an weiteren zur Laufzeit konfigurierbaren Sitzungseinstellungen vor, so werden diese Änderungen in den dafür zugeordneten Variablen innerhalb des Session Contextes nachvollzogen.

[0154] Bei einem Logoff wird der Session Context entsprechend gelöscht. Nachfolgende Prüfungsaufrufe mit dieser Session ID werden abgewiesen.

[0155] Die Verwaltung von Benutzern und Passwörtern ist in einem allgemeinen Benutzerverwaltungskonzept für bevorzugte Entgeltsicherung zu definieren, das Bestandteil des Feinkonzeptes bevorzugte Entgeltsicherungs-IT ist.

[0156] Die Lesesysteme müssen sich vor der Durchführung von Prüfungsanfragen bei dem Validation Controller registrieren lassen. Als Parameter ist die ID des Lesesystems sowie ein Passwort zu übergeben. Als Rückgabewert wird bei erfolgreicher Anmeldung ebenfalls eine Session ID zurückgeliefert, die bei den folgenden Überprüfungsanfragen zu übermitteln ist.

[0157] Bei einem Shutdown des Lesesystems muss ein entsprechender Logoff mit dieser Session ID erfolgen.

Sonstiges

Spezielle Benutzerrollen

[0158] Im Rahmen des Sicherheitskonzepts sind zwei spezielle Benutzerrollen vorzusehen, die von zwei unterschiedlichen Personen auszufüllen sind.

Der/die Sicherheitsadministrator(in)

[0159] Die Rolle der Sicherheitsadministration umfasst die folgenden Aufgaben:

- Erstellung von Befehlsdateien zur Administration der Krypto-Karte
- Signierung dieser Befehlsdateien
- Initialisierung und Verwaltung der Krypto-Karten
- Kontrolle der aufzuspielenden Software und der zugehörigen Konfiguration

[0160] Der Sicherheitsadministrator authentisiert sich mit dem Private Key zur Kartenadministration. Dieser ist auf einer Diskette oder Smart Card gespeichert und muss von dem Sicherheitsadministrator streng unter Verschluss gehalten werden.

[0161] Nur mit diesem Schlüssel signierte Administrationsbefehle lassen sich auf der Krypto-Karte ausführen. Da durch diesen Mechanismus die Befehlssequenz und die zugehörigen Parameter geschützt sind, kann die Ausführung die-

ser Befehle auch an Systemadministratoren vor Ort delegiert werden. Der Sicherheitsadministrator muss dazu die Befehle zur Verfügung stellen und eine entsprechende Verfahrensanweisung schreiben.

[0162] Eine weitere Aufgabe besteht in der Verwaltung der Krypto-Karten, wobei zu jeder Karte die Seriennummer, die Konfiguration und die Systemnummer des Systems, in welchem diese installiert sind, sowie der Standort des Systems festgehalten werden. Bei den Reserve-Krypto-Karten wird ferner festgehalten, in wessen Besitz sich die Karten befinden.

[0163] Zusammen mit dem QS-Manager Sicherheit kontrolliert er die Softwarequellen und die zugehörige Softwarekonfiguration und gibt diese zur Installation frei.

[0164] Außerdem erfolgt eine Prüfung der auf der Karte und auf dem Krypto Server zu installierenden, beziehungsweise installierten, Software sowie eine Freigabe und Signierung der Kartensoftware.

[0165] Die Kartensoftware ist speziell daraufhin zu prüfen, ob an irgendeiner Stelle einer der geheimen Schlüssel über die Treiberschnittstelle nach außen gegeben werden kann, beziehungsweise ob dort Manipulationsversuche wie zum Beispiel die Speicherung konstanter vordefinierter Schlüssel oder die Verwendung unsicherer Verschlüsselungsverfahren vorgenommen wurden. Zusätzlich zur Kartensoftware ist auch die mit ihr in Verbindung stehende Anwendungssoftware des Krypto Servers zu prüfen.

[0166] Die Authentisierung erfolgt genauso wie bei dem Sicherheitsadministrator mit einem Private Key. Es handelt sich hierbei jedoch um den Private Key zur Softwaresignierung.

[0167] Es besteht hier jedoch eine zusätzliche Sicherheit darin, dass zur Installation der Software nicht nur die Software zu signieren ist, sondern auch der zugehörige Installationsbefehl. Da hierfür zwei verschiedene Personen (Qs-Manager und Sicherheitsadministrator) zuständig sind und dadurch, dass die zugehörigen Schlüssel an zwei unterschiedlichen Orten aufbewahrt werden, ist hier ebenfalls eine hohe Sicherheit gewährleistet.

[0168] Die Distribution der Software wird von dem QS-Manager Sicherheit in Abstimmung mit dem Sicherheitsadministrator vorgenommen.

[0169] Diese besonders bevorzugte Ausführungsform der Erfindung sieht somit zwei verschiedene Authentisierungsschlüssel vor, so dass die Datensicherheit erheblich erhöht wird.

Patentansprüche

1. Verfahren zur Überprüfung der Echtheit eines auf einer Postsendung aufgebrachten Freimachungsvermerks, wobei in dem Freimachungsvermerk enthaltene kryptographische Informationen entschlüsselt und zur Überprüfung der Echtheit des Freimachungsvermerkes eingesetzt werden, **dadurch gekennzeichnet**, dass die Leseeinheit den Freimachungsvermerk graphisch erfasst und an eine Überprüfungseinheit übermittelt, und dass die Überprüfungseinheit einen Ablauf von Teilprüfungen steuert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine der Teilprüfungen die Entschlüsselung der in dem Freimachungsvermerk enthaltenen kryptographischen Informationen beinhaltet.

3. Verfahren nach einem oder beiden der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass eine der Teilprüfungen einen Vergleich zwischen dem Erzeugungsdatum des Freimachungsvermerkes und dem aktuellen Datum beinhaltet.

4. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Leseeinheit und die Überprüfungseinheit mittels eines synchronen Protokolls Informationen austauschen.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass das Protokoll RPC basiert ist.

6. Verfahren nach einem oder mehreren der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Leseeinheit und die Überprüfungseinheit über ein asynchrones Protokoll miteinander kommunizieren.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass die Leseeinheit ein Datentelegramm an die Überprüfungseinheit sendet.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass das Datentelegramm den Inhalt des Freimachungsvermerks enthält.

9. Verfahren nach einem oder mehreren der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass das Datentelegramm eine Anforderung zum Starten einer kryptographischen Überprüfungsroutine enthält.

10. Verfahren nach einem oder mehreren der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass durch ein Krypto-Interface eine Lastverteilung zwischen mehreren Überprüfungsmitteln erfolgt.

11. Verfahren nach einem oder mehreren der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der Inhalt des Freimachungsvermerks in einzelne Felder aufgeteilt wird.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass eine Identifikationsnummer (Postage ID) des die Erzeugung des Freimachungsvermerks steuernden Kundensystems aus dem Freimachungsvermerk ermittelt wird.

13. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass einzelne Kundensystemidentifikationsangaben (Postage ID) in einer Negativdatei erfasst und die zu dieser Postage ID gehörenden Sendungen aus einem normalen Bearbeitungsverlauf von Postsendungen ausgeschleust werden.

14. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass eine in dem Freimachungsvermerk enthaltene verschlüsselte Angabe einer Empfängeradresse mit einer für die Beförderung der Postsendung angegebenen Empfängeradresse verglichen wird.

15. Verfahren nach einem oder mehreren der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass Überprüfungsparameter des Verfahrens geändert werden können.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, dass eine Änderung von Verfahrensparametern nur nach Eingabe eines persönlichen digitalen Schlüssels (Private Key) eines Systemadministrators erfolgt.

Hierzu 7 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 31 254 A1
Int. Cl.[7]: H04L 9/00
Offenlegungstag: 23. Januar 2003

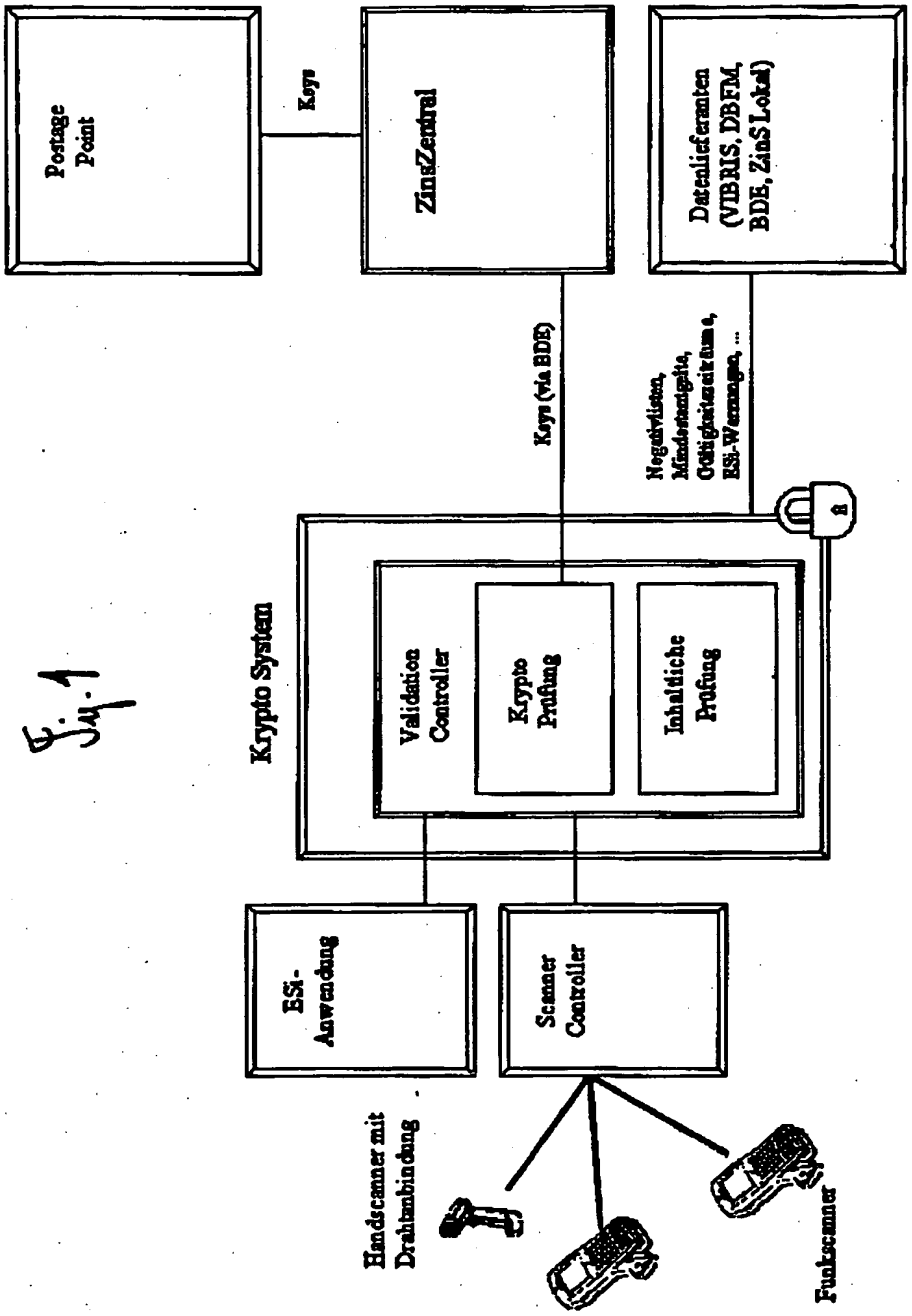
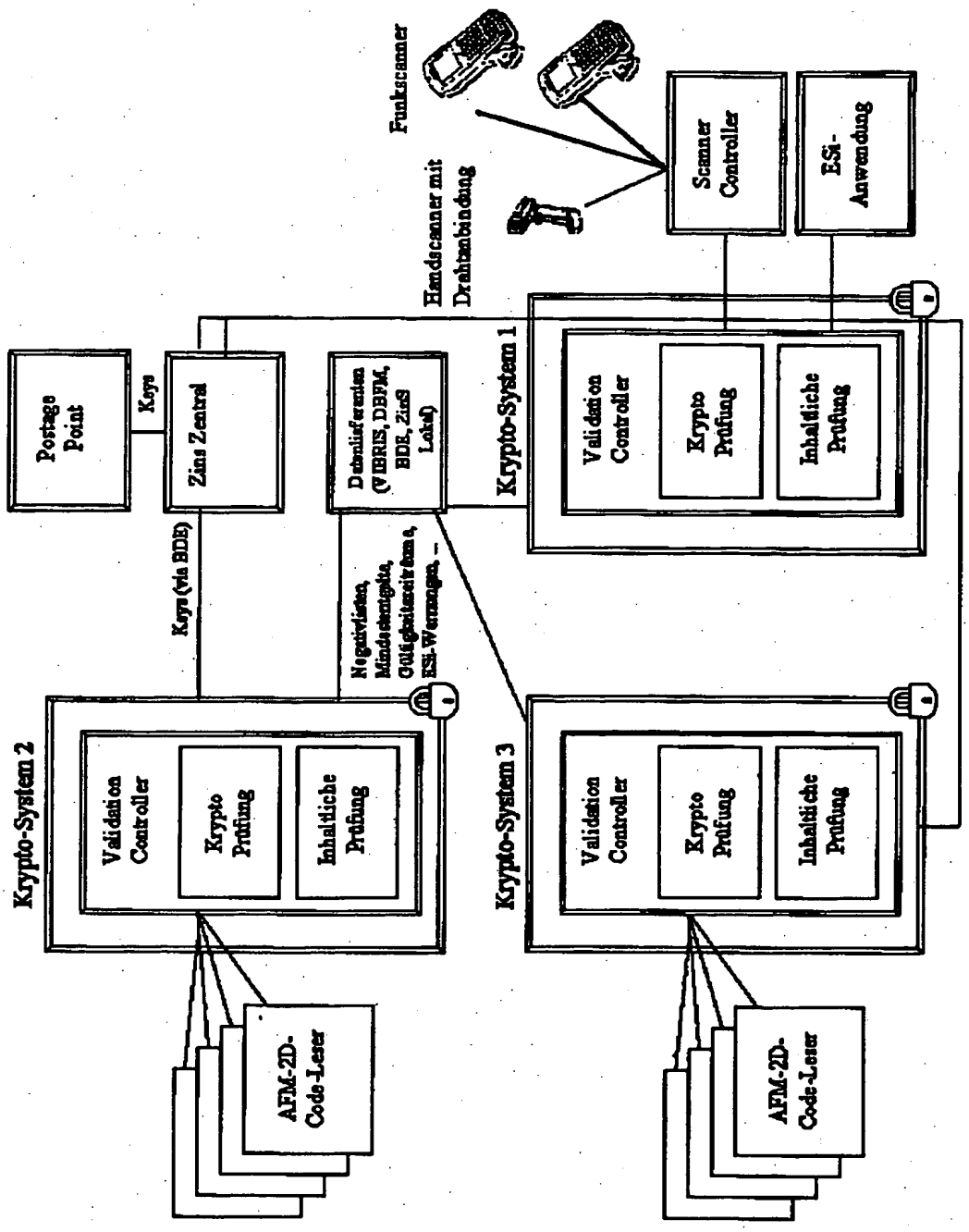


Fig. 1

Nummer: DE 101 31 254 A1
Int. Cl.[7]: H04L 9/00
Offenlegungstag: 23. Januar 2003

Fig. 1



Nummer: DE 101 31 254 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 23. Januar 2003

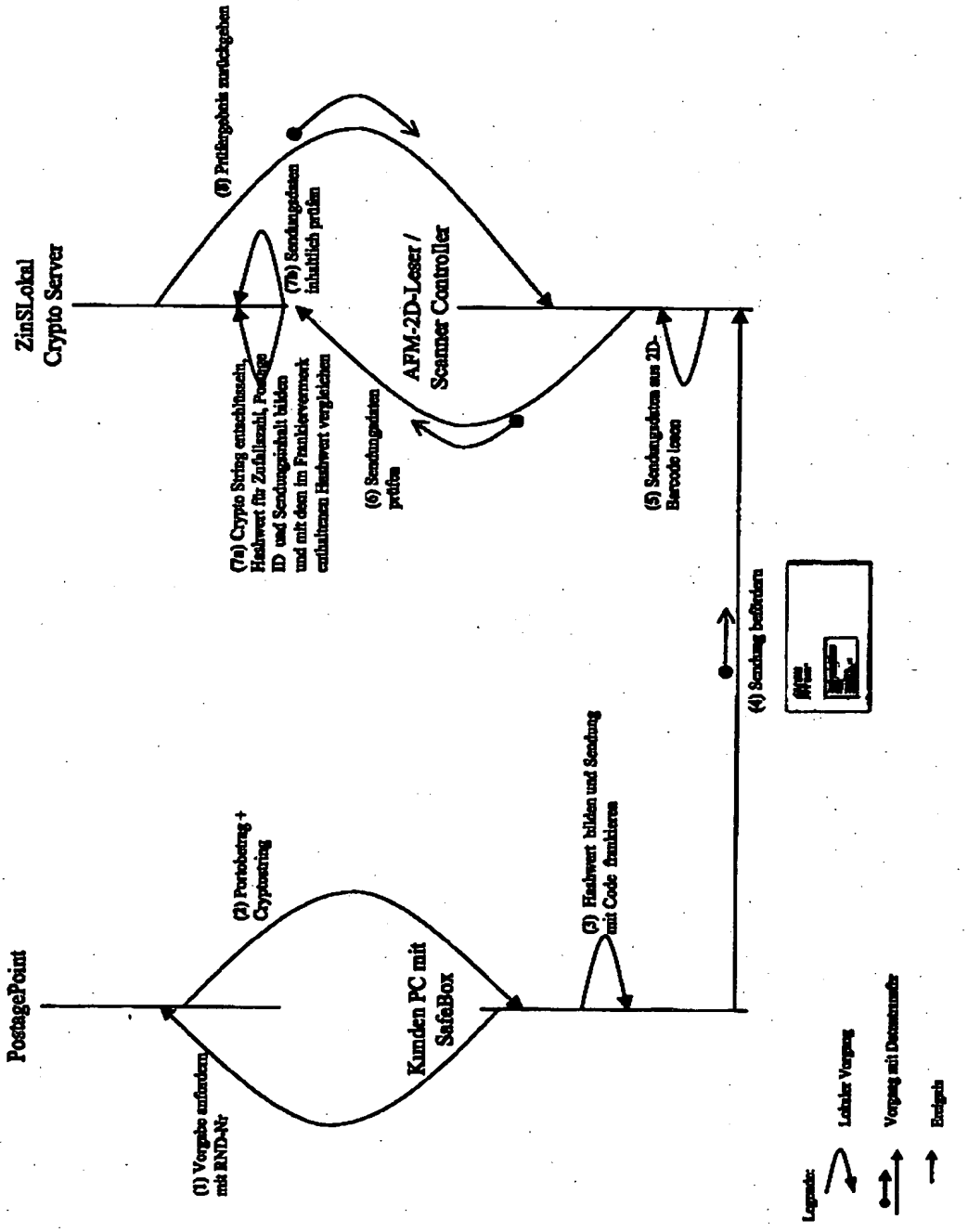
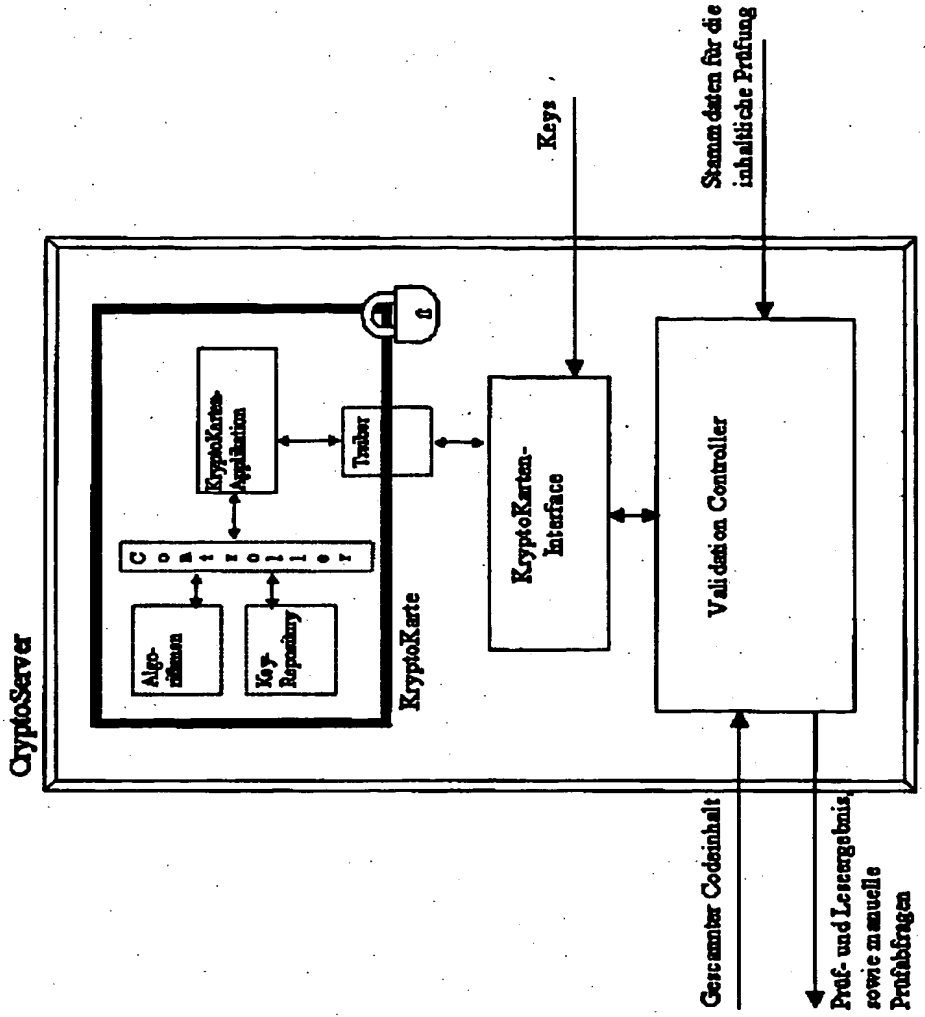


Fig. 3

Nummer: DE 101 31 254 A1
Int. Cl.[7]: H04L 9/00
Offenlegungstag: 23. Januar 2003



Nummer: DE 101 31 254 A1
Int. Cl.[7]: H04L 9/00
Offenlegungstag: 23. Januar 2003

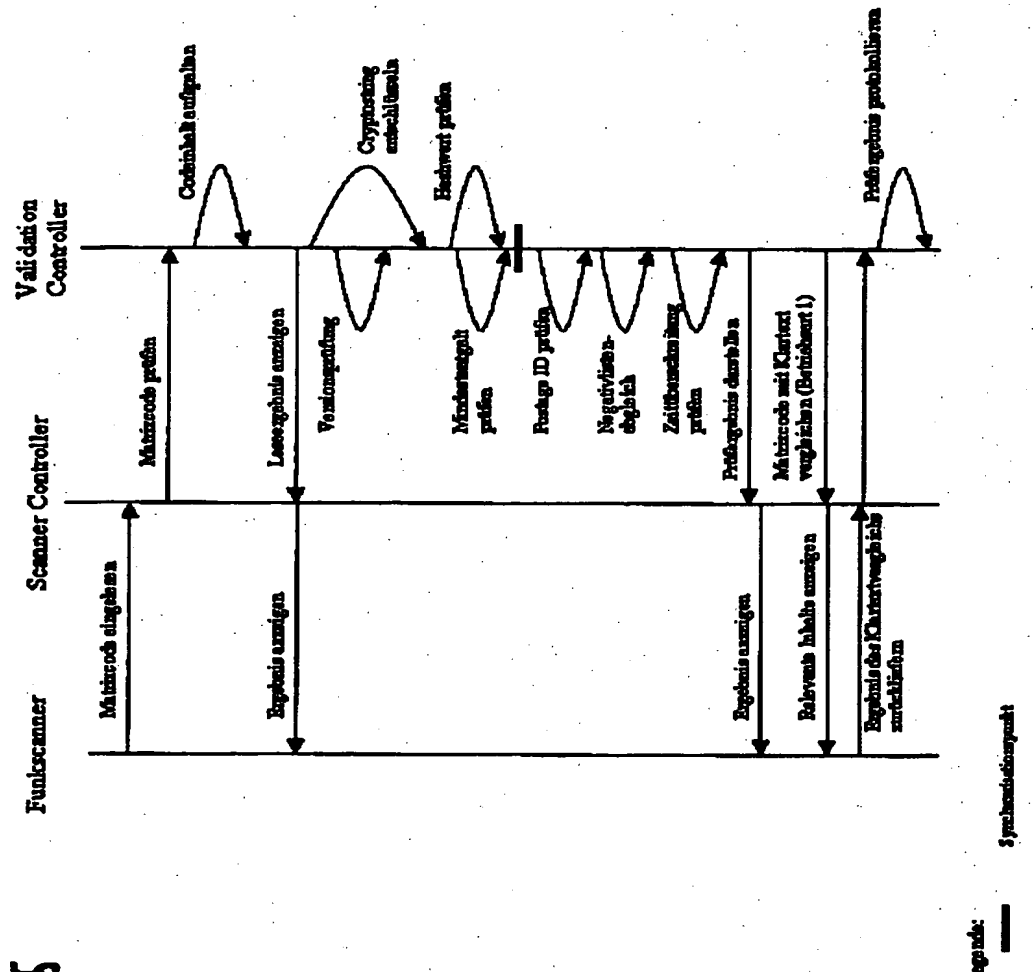
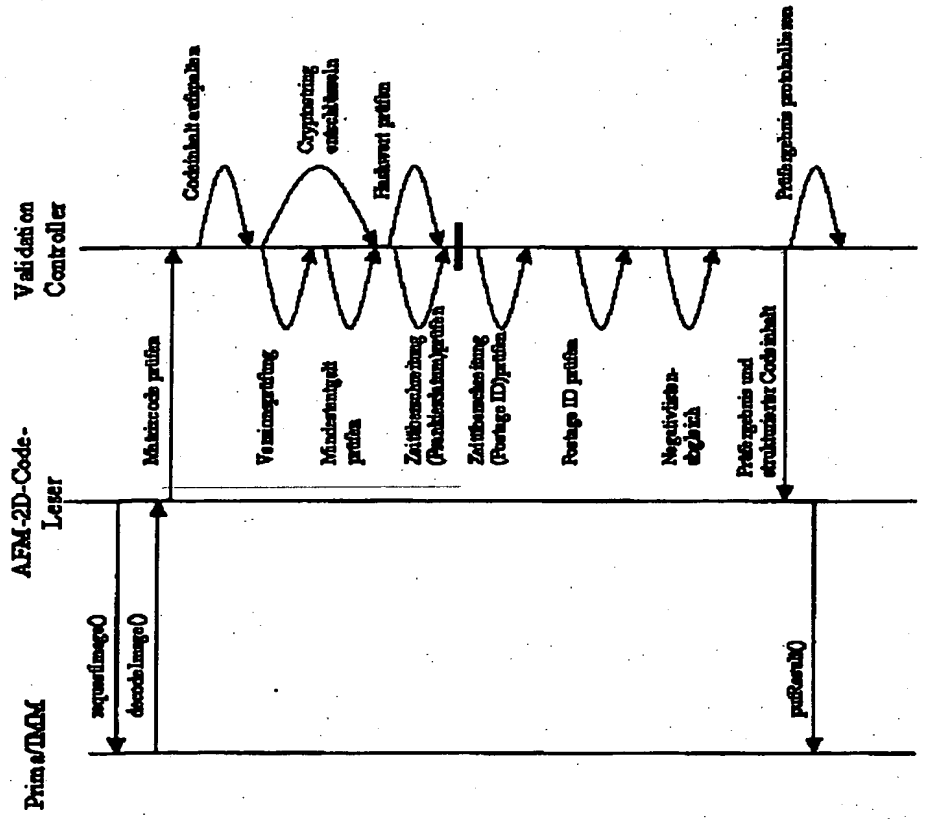


Fig. 5

Nummer: DE 101 31 254 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 23. Januar 2003



Legende: — Synchronisationspunkt

Fig. 6

Nummer: DE 101 31 254 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 23. Januar 2003

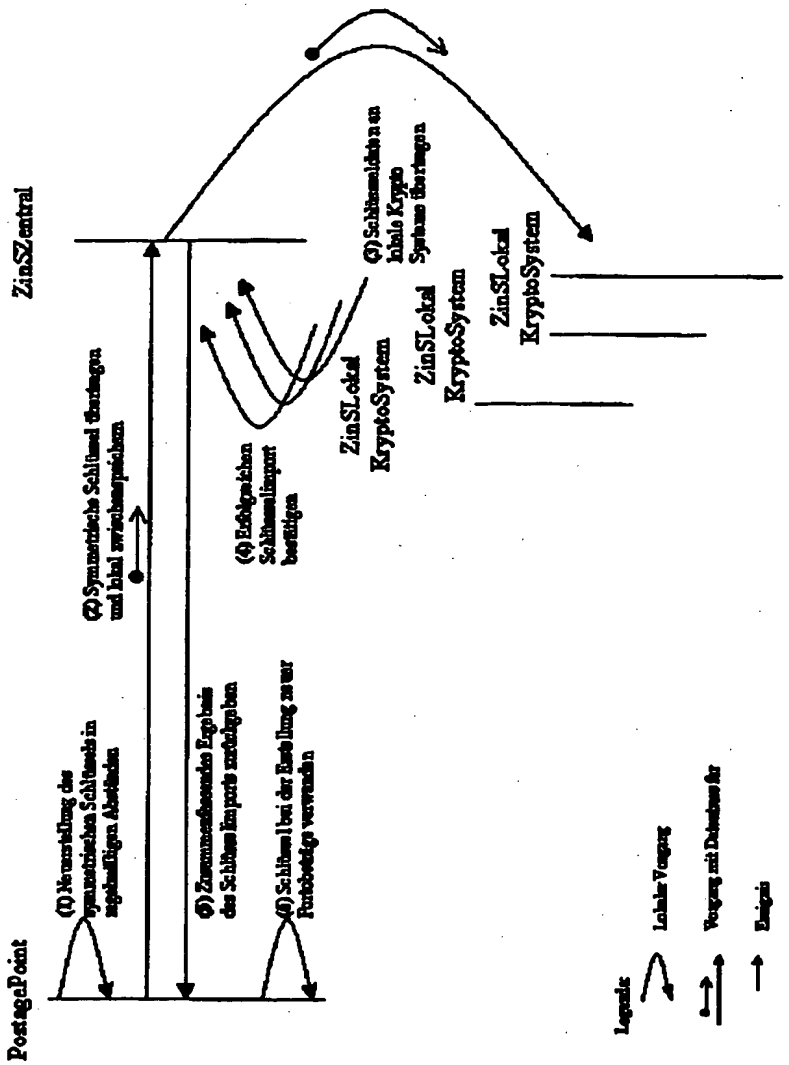


Fig. 1